PROGRAM FOR COMMUNITY DETECTION AND DISCLOSURE OF VULNERABILITIES

Securing Email and Digitizing Workflows

RPost is a global leader in secure and certified electronic communications, built upon its patented RMail®, RSign®, and Registered Email™ delivery proof, email encryption, e-security, and e-signature technologies. Millions of users have enjoyed RPost services in more than 100 countries, since 2000.

RPost accepts reports of any vulnerability of our services.

Vulnerability Disclosure Program Scope

RPost's Vulnerability Disclosure Program initially covers the following products:

- RMail® Registered Email™ service
- RMail® encrypted email service
- RMail®, RSign®, RForms™ e-signature services and features
- RMail Gateway™ services
- RMail® e-security and file share services and features

Legal Posture

The RPost corporate entities and affiliates will not engage in legal action against individuals who submit vulnerability reports for their activities in identifying and reporting the vulnerability, such activities consisting of:

- Engaging in the testing of systems/research without harming RPost or its customers.
- Engaging in vulnerability testing within the scope of our vulnerability disclosure program that do not diminish services availability to customers.
- Testing on products without affecting customers, or after receipt of permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhering to the laws of their location and the location of RPost corporate entities and affiliates. For example, violating laws that would only result in a claim by RPost (and not a criminal claim) may be acceptable as RPost is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public.

How to Submit a Vulnerability

Vulnerability Reports should be submitted to vulnerability@rpost.com. The report email should:

- Include "Vulnerability Report" in the subject line.
- Include contact information for the person/organizations submitting the report.
- Identify the RPost service in which the vulnerability was discovered.
- The time and date of the testing that revealed the vulnerability.
- Describe the nature of the vulnerability in sufficient detail to allow RPost's Security team to replicate the vulnerability.
- If possible, suggestions for possible remediation of the vulnerability.

Acceptance Criteria

RPost will not accept a vulnerability report unless it contains information sufficient for RPost's security team to duplicate the vulnerability. If the vulnerability is triggered by a particular format or form of message or attachment, a copy of the relevant message or attachments should be included. If the vulnerability was detected using a password protected RPost service, the report should include the username under which the tests were conducted.

Our Commitment

Researchers reporting a vulnerability may expect:

- Each submission will be reviewed by RPost technology teams.
- After analysis, if the reported issue merits an action, RPost shall offer a complimentary RMail annual service license for personal use as an indication of gratitude for the researcher's efforts.

Last Update: 201215